AO 106 (Rev. 04/10) Application for a Search Warrant

United States District Court

for the
Western District of New York

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address.)

A Samsung Galaxy cellular telephone, serial number RF8M73W5EJZ, in the care and custody of Homeland Security Investigations located at 250 Delaware Avenue, 8th Floor, Buffalo NY 14202

Case No. 19-MJ-1144

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

This warrant applies to information associated with SUBJECT PHONE, Samsung Galaxy cellular telephone, serial number RF8M73W5EJZ, described further in Attachment A, which is attached hereto and incorporated by reference herein.

Located in the Western District of New York, there is now concealed *(identify the person or describe the property to be seized)*:
Evidence, fruits and instrumentalities pertaining to violations of Title 18, United States Code, Section 2252A(a)(2)(A) and 2252A(a)(5)(B), as more fully set forth in Attachment B, which is attached hereto and incorporated by reference herein.

The basis for search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of Title 18, United States Code, Section 2252A(a)(2)(A) and 2252A(a)(5)(B).

The application is based on these facts:

- ☒ continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

KAREN L. WISNIEWSKI
SPECIAL AGENT
HOMELAND SECURITY INVESTIGATIONS
Printed name and title

Sworn to before me and signed in my presence.

Date: December 9, 2019

Judge's signature

HONORABLE JEREMIAH J. MCCARTHY
UNITED STATES MAGISTRATE JUDGE
Printed name and Title

City and state: Buffalo, New York

AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR A SEARCH WARRANT

I, **KAREN L. WISNIEWSKI**, being duly sworn, depose and state the following:

I. INTRODUCTION & AGENT BACKGROUND

1. I am a Special Agent with Homeland Security Investigations (HSI) and have been so employed since March 2003. Prior to that, I was employed as a Special Agent with the United States Customs Service since 1998. I am currently assigned to the Buffalo Field Office of HSI and am assigned to the Child Exploitation Unit (CEU). As a member of the CEU, I investigate the sexual exploitation of children, including the production, distribution, receipt, and possession of child pornography, coercion/enticement, and the transfer of obscene material to minors in violation of Title 18, United States Code, Sections 2251, 2252, 2252A, 2422, and 1470. I have received specialized training in the area of child pornography, child exploitation, coercion/enticement, and I've had the opportunity to observe and review numerous examples of child pornography, as defined in Title 18, United States Code, Section 2256.

2. This affidavit is submitted pursuant to Rule 41 of the Federal Rules of Criminal Procedure in support of an application for a search warrant for a **Samsung Galaxy cellular telephone identified by** serial **number RF8M73W5EJZ** (hereinafter the "SUBJECT PHONE"). The SUBJECT PHONE is more particularly described in **Attachment A** of this Affidavit. The item to be searched is anticipated to possess evidence related the possession,

receipt, and distribution of child pornography in violation of 18 U.S.C. §§ 2252A(a)(2)(A) and 2252A(a)(5)(B), as more specifically described in **Attachment B** of this Affidavit.

3. The statements in this affidavit are based in part on information provided to me by other law enforcement officers and my investigation of this matter. Since this affidavit is submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth facts sufficient to establish probable cause that contraband, evidence, fruits and instrumentalities involving the possession, receipt, and distribution of child pornography are presently located on the SUBJECT PHONE.

II. RELEVANT STATUTES

4. Pursuant to Title 18, United States Code, Section 2252A(a)(2)(A), it is a federal crime for any person to knowingly receive or distribute any child pornography that has been mailed, or shipped or transported in interstate or foreign commerce by any means, including by computer.

5. Pursuant to Title 18, United States Code, Section 2252A(a)(5)(B), it is a federal crime for any person to knowingly possess child pornography and knowingly access with intent to view, any material that contains images of child pornography that has been mailed or, using any means or facility of interstate or foreign commerce, has been shipped or transported in or affecting interstate or foreign commerce by any means, including by computer and that the images were produced using materials that have been mailed, shipped

or transported in or affecting interstate of foreign commerce by any means including computer.

III. THE INVESTIGATION AND FACTUAL BASIS

6. In August 2018, a rose-gold Apple iPhone 8 was turned into the New York State Police ("NYSP") Barracks in Niagara Falls, NY. The individual who brought the iPhone to the NYSP informed investigators that she had found the iPhone in a park in the City of Niagara Falls and that she had observed conversations on the phone discussing sexual intercourse with minor children and observed images of young boys naked in bath tubs on the phone.

7. An investigation by the NYSP based upon information found on the iPhone and law enforcement checks determined that an individual named JEREMY SPEARS, date of birth January 17, 1998, was the owner of the iPhone.

8. On or about May 14, 2019, Niagara Falls City Court Judge James J. Faso authorized a search warrant to search the contents of the iPhone. Pursuant to this warrant, the Niagara Falls Police Department Forensic Unit conducted a forensic examination of the iPhone. This examination revealed that the iPhone contained Twitter chats discussing sexual intercourse with minor children and contained approximately 50 images of child pornography. Your Affiant viewed the images recovered from the iPhone and confirmed the presence of multiple images of suspected child pornography (as defined in Title 18, United States Code, Section 2256). These images include the following:

a. The first file is an image with the file path "iphone/var/mobile/Media/Photodata/Thumbnails/V2/Photodata/CPLAssets/group90/1110C3E3-CB91-4FEA-B862-845AD0797BFCJPG/5003.JPG/5003.jpg_embedded_1.jpg. This image depicts a nude pubescent minor male laying on a couch with his legs spread open. His pants and underwear are off and the focus of the image is his naked penis.

b. The second file is an image with the file path "iphone/var/mobile/Media/Photodata/Thumbnails/V2/Photodata/CPLAssets/group481/0BB95639-92B8-4292-AA95-Fcc35CE0388D.JPG/5003.JPG/5003.JPG_embedded_1.jpg" This image depicts a prepubescent minor male child lying naked on a bed with the focus being on his naked penis.

c. The third file is an image with a file path "iphone/var/mobile/Media/Photodata/Thumbnails/V2/Photodata/CPLAssets/group442/1B913E94-4B5A-4F69-B204-A9D133232FC6.JPG/5003.jpg/5003.JPG_embedded_1.jpg. This image depicts a naked prepubescent boy kneeling with his hand on his hip and the focus being his penis.

9. On November 1, 2019, JEREMY SPEARS gave a Mirandized statement to New York State Police Investigators at the NYSP Barracks in Niagara Falls, New York. At the time, SPEARS was in possession of a Samsung Galaxy cellular telephone, the SUBJECT PHONE. In his statement, SPEARS stated that he had actively searched for images of child pornography using internet search engines Tumblr and Google using the SUBJECT PHONE. SPEARS admitted that he has an addiction to child pornography and looks at it on the SUBJECT PHONE 3 to 4 times a week.

10. SPEARS stated that he has shared images of child pornography with other individuals over the internet. Additionally, SPEARS stated that in, addition to viewing the images of child pornography, he had engaged in hands-on sexual conduct with a minor child in West Virginia. SPEARS further stated that he wanted to "get rid of the stuff" on the SUBJECT PHONE, referencing the images of child pornography and stated that there were approximately 20 to 30 images of child pornography on the SUBJECT PHONE.

11. On November 1, 2019, SPEARS signed a New York State Police Voluntary Consent to Search Form authorizing a search of the SUBJECT PHONE. SPEARS also provided NYSP investigators with his password. NYSP Investigator Donald Ginnane secured the SUBJECT PHONE at the NYSP Barracks.

12. On November 1, 2019, SPEARS was charged, by way of felony complaint, with five counts of Possession of Sexual Performance by a Child (New York State Penal Law § 263.16) and five counts of Promoting the Sexual Performance of a Child (New York State Penal Law § 263.15) in Niagara Falls City Court based upon images recovered from the iPhone. On November 2, 2019, SPEARS was arraigned in Niagara County City Court. Bail was set in the amount of $10,000 bond or $20,000 cash. Defendant is currently incarcerated at the Niagara County jail.

13. Your Affiant is submitting this application for a warrant to search SUBJECT PHONE, as further described in Affidavit A. On November 12, 2019, NYSP Investigators

gave your affiant custody of the SUBJECT PHONE. An HSI chain of custody was initiated and the SUBJECT PHONE was electronically secured by placing SUBJECT PHONE in airplane mode so that it cannot be remotely erased. The SUBJECT PHONE was secured in the HSI Forensic Lab located at 250 Delaware Avenue, Buffalo, NY and has remained in the custody and care of HSI Buffalo since it was received on November 12, 2019.

14. Based on the forgoing, there is probable cause to believe that evidence, fruits, or contraband in violation of Title 18, United States Code, Section 2252A(a)(2)(A) and 2252A(a)(5)(B) will be found in the SUBJECT PHONE, as described in Attachment A.

IV. TRAINING AND EXPERIENCE

15. Based upon my training and experience, computers, hard drives, removable media and other electronic devices have the capacity to retain information, even after that information has been deleted by the user. Thus, images, videos and other files including correspondence in the form of emails, chat logs, and records associated with coercion, enticement, promotion of sexual activity, as well as the production, receipt, distribution and possession of child pornography may be recovered from electronic and digital media, even if those files were previously deleted.

16. Based on my training, experience, and knowledge, and the experience of other law enforcement personnel involved in this investigation, I know that the Internet is a worldwide computer network that connects computers and allows communications and the transfer of data and information across state and national boundaries. Computer technology

and the Internet revolutionized the way in which child pornography is produced, distributed, stored and communicated as a commodity and a further tool of child exploitation. For instance:

a. Individuals can transfer photographs from a camera onto a computer-readable format with a variety of devices, including scanners, memory card readers, or directly from digital cameras, including those on most cellphones.

b. Modems allow computers to connect to another computer through the use of telephone, cable, or wireless connection. Electronic contact can be made to literally millions of computers around the world.

c. The capability of a computer to store images in digital form makes the computer itself an ideal repository for child pornography. As explained further below, personal ownership and quantity of electronic media in use worldwide, and the storage capacity of home computers and other media, have increased tremendously in the last decade and continue to grow. Computer drives and other electronic storage media can store a huge amount of visual images at very high resolution.

d. The Internet, the World Wide Web and other Internet components afford individuals many different and relatively secure and anonymous venues for obtaining, viewing and trading child pornography or for communicating with others to do so or to entice children.

e. Individuals can use online resources to retrieve, store and share child pornography, including services offered by Internet Portals such as Google, America Online (AOL), Yahoo! and Hotmail, among others. Online services allow a user to set up an account providing e-mail and instant messaging services, as well as electronic storage of computer files in any variety of formats. A user can set up an online storage account from any computer or cellular phone with access to the Internet. Evidence of such online storage of child pornography is often found on the user's computer. Even in cases where online storage is used, evidence of child pornography can be found on the user's computer in most instances.

f. As is the case with most digital technology, computer communications can be saved or stored on hardware and computer storage media used for these purposes. Storing this information can be intentional, i.e., by saving an e-mail as a file on the computer or saving the location of one's favorite web sites in, for example, bookmarked files. However, digital

information can also be retained unintentionally, e.g., traces of the path of an electronic communication may be automatically stored in many places (e.g., temporary files or ISP client software, among others). In addition to electronic communications, a computer user's Internet activities generally leave traces or footprints in the web cache and history files of the browser used. Such information is often maintained for very long periods of time until overwritten by other data.

g. The interaction between software applications and the computer operating systems often results in material obtained from the Internet being stored multiple times, and even in different locations, on a computer hard drive without the user's knowledge. Even if the computer user is sophisticated and understands this automatic storage of information on his computer's hard drive, attempts at deleting the material often fail because the material may be automatically stored multiple times and in multiple locations within the computer media. As a result, digital data that may have evidentiary value to this investigation could exist in the user's computer media despite, and long after, attempts at deleting it. A thorough search of this media could uncover evidence of receipt, distribution and possession of child pornography.

h. Data that exists on a computer is particularly resilient to deletion. Computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted or viewed via the Internet. Electronic files downloaded to a hard drive can be stored for years at little to no cost. Even when such files have been deleted, they can be recovered months or years later using readily-available forensic tools. When a person deletes a file on a home computer, the data contained in the file does not actually disappear, rather, the data remains on the hard drive until it is overwritten by new data. Therefore, deleted files or remnants of deleted files, may reside in free space or slack space, that is, in space on the hard drive that is not allocated to an active file and is left unused and free to store new data. Such residual data may remain in free space for long periods of time before it is overwritten by new data. In addition, a computer's operating system may also keep a record of deleted data in a swap or recovery file. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or cache. The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity and computer habits.

17. In addition, based on my training and experience, and the training and experience of other law enforcement officers with whom I have had discussions, I have learned that individuals who produce, distribute/receive, and possess child pornography are often individuals who have a sexual interest in children and in images of children, and that there are certain characteristics common to such individuals:

a. Individuals who have a sexual interest in children or images of children may receive sexual gratification, stimulation, and satisfaction from contact with children; or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or in other visual media; or from literature describing such activity.

b. Individuals who have a sexual interest in children or images of children may collect sexually explicit or suggestive materials, in a variety of media including online accounts and devices such as the SUBJECT PHONE. Individuals who have a sexual interest in children or images of children oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

c. Likewise, individuals who have a sexual interest in children or images of children often maintain their collections that are in a digital or electronic format in a safe, secure, and private environment, such as a computer or on an online account, or on smart phones such as the SUBJECT PHONE. These collections are kept to enable the individual to view the collection, which is valued highly.

d. Individuals who have a sexual interest in children or images of children also may correspond with and/or meet others to share information and materials; conceal such correspondence as they do their sexually explicit material; and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.

e. Individuals who have a sexual interest in children or images of children prefer not to be without their child pornography for any prolonged time

period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world.

f. Individuals can use online resources to retrieve, store and share child pornography, including services offered by Internet Portals such as Google, America Online (AOL), Yahoo! and Hotmail, among others, all of which can be accessed by the SUBJECT PHONE. Online services allow a user to set up an account providing e-mail and instant messaging services, as well as electronic storage of cellular telephone files in any variety of formats. A user can set up an online storage account from any cellular telephone with access to the Internet. Evidence of such online storage of child pornography is often found within the device used to access the account, such as the SUBJECT PHONE.

V. BACKGROUND ON COMPUTERS AND EVIDENCE ASSESSMENT PROCESS IN CHILD PORNOGRAPHY AND CHILD EXPLOITATION INVESTIGATION

18. This warrant seeks permission to locate not only computer files that might serve as direct devices were used, the purpose of their use, and who used them.

19. As described above, and in Attachment B, this application seeks permission to search and seize certain digital evidence that might be found in the SUBJECT PHONE, in whatever form it is found. One form in which the records might be found is stored on a computer's hard drive, mobile computing device, or other electronic media. Some of these electronic records might take the form of files, documents, and other data that is user-generated. Some of these electronic records, as explained below, might take a form that becomes meaningful only upon forensic analysis. In addition to user-generated documents (such as messages, picture and movie files), computing devices can contain other forms of electronic evidence that are not user-generated. In particular, a computing device may

contain records of how a computer or mobile device has been used, the purposes for which it was used and who has used these records, as described further in the attachments.

20. Based upon my knowledge, training, and experience, as well as information related to me by agents and others involved in the forensic examination of digital devices, I know that segregating information before commencement of the review of digital evidence by the examining agent is inconsistent with the evidence assessment process in child pornography and online child exploitation investigations. This is true in part because the items to be searched will not only contain child pornography, but also will contain the identity of the user/possessor of the child pornography as well as evidence as to the programs and software used to obtain the child pornography, which may be located throughout the areas to be searched. In addition, it is not possible to know in advance which computing device or storage media will contain evidence of the specified crimes, and often, such evidence is contained on more than one computer/device or digital storage device. Further:

a. Searching digital devices can be a highly technical process that requires specific expertise, specialized equipment and knowledge of how electronic and digital devices are often used in child pornography and online child exploitation matters. There are so many types of digital devices and software in use today that it is impossible to bring to the search site all of the necessary technical manuals and specialized equipment necessary to conduct a thorough search.

b. Because of the numerous types of digital devices and software that may contain evidence in child pornography and online child exploitation cases, it may also be necessary to consult with specially trained personnel who have specific expertise in the type of digital device, software application or operating system that is being searched in an off-site and controlled laboratory environment.

c. Because digital data is particularly vulnerable to inadvertent or intentional modification or destruction, searching digital devices can

require the use of precise, scientific procedures that are designed to maintain the integrity of digital data and to recover "hidden," erased, compressed, encrypted or password-protected data. Data hiding analysis can be useful in detecting and recovering such data and may indicate knowledge, ownership, or intent. The recovery of "hidden" data is highly specialized and time-intensive. For this reason, on-site key word searches are not sufficient to recover inadvertently or intentionally modified or destroyed data. Similarly, running hash values on-site to find files that contain child pornography is not an adequate on-site review and seizure procedure, because while hash values locate previously identified files of child pornography, they do not capture files that are the result of new production, images imbedded in an alternative file format, or images altered, for instance, by a single pixel. As a result, a controlled environment, such as a law enforcement laboratory, is essential to conducting a complete and accurate analysis of data stored on digital devices.

d. The volume of data stored on many digital devices will typically be so large that it will be highly impractical to search for data during the execution of the physical search of the premises. A single megabyte of storage space is the equivalent of 500 double-spaced pages of text. A single gigabyte of storage space, or 1,000 megabytes, is the equivalent of 500,000 double-spaced pages of text. Storage devices capable of storing 500 gigabytes (GB) of data are now commonplace in desktop computers. Consequently, each non-networked, desktop computer found during a search can easily contain the equivalent of 240 million pages of data. Further, a 500 GB drive could contain as many as approximately 450 full run movies or 450,000 songs. As examining this quantity of data can take weeks or months, depending on the volume of the data stored, it would be impractical to attempt this kind of data search on-site.

e. Electronic files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted or viewed via the Internet. Electronic files saved to a hard drive can be stored for years with little or no cost. Even when such files have been deleted, they can be recovered months or years later using readily-available forensics tools. Normally, when a person deletes a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or cache. The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are

replaced with more recently viewed Internet pages. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer habits. Recovery of residue of electronic files from a hard drive requires specialized tools and a controlled laboratory environment.

f. Digital device users can attempt to conceal data within digital devices through a number of methods, including the use of innocuous or misleading filenames and extensions. For example, files with the extension ".jpg" often are image files; however, a user can easily change the extension to ".txt" to conceal the image and make it appear that the file contains text. Digital device users may also attempt to conceal data by using encryption, which means that a password or physical device, such as a "dongle" or "keycard," is necessary to decrypt the data into readable form. In addition, digital device users can conceal data within another seemingly unrelated and innocuous file in a process called "steganography." For example, by using steganography, a digital device user can conceal text in an image file that cannot be viewed when the image file is opened. "Digital devices may also contain "booby traps" that destroy or alter data if certain procedures are not scrupulously followed." A substantial amount of time is necessary to extract and sort through data that is concealed, encrypted, or subject to booby traps, to determine whether it is evidence, contraband or instrumentalities of a crime.

g. Further, in finding evidence of how a computer has been used, the purposes for which it was used, and who has used it, sometimes it is necessary to establish that a particular thing is not present on a hard drive or that a particular person (in the case of a multi-user computer) was not a user of the computer during the time(s) of the criminal activity. For instance, based upon my knowledge, training, and experience, as well as information related to me by agents and others involved in the forensic examination of digital devices, I know that when a computer has more than one user, files can contain information indicating the dates and times that files were created as well as the sequence in which they were created, so that evidence of whether a user accessed other information close in time to the file creation dates, times and sequences can help establish user identity and exclude other users from computer usage during relevant times.

h. Because the absence of particular data on a digital device may provide evidence of how a digital device has been used, what it has been used for,

and who has used it, analysis of the digital device as a whole may be required to demonstrate the absence of particular data. Such evidence of the absence of particular data on a digital device is not segregable from the digital device.

i. The types of evidence described above may be direct evidence of a crime, indirect evidence of a crime indicating the location of evidence or a space where evidence was once located, contextual evidence identifying a computer user, and contextual evidence excluding a computer user. All of these types of evidence may indicate ownership, knowledge, and intent. This type of evidence is not "data" that can be segregated, that is, this type of data cannot be abstractly reviewed and filtered by a seizing or imaging agent and then transmitted to investigators. Rather, evidence of this type is a conclusion, based on a review of all available facts and the application of knowledge about how a computer behaves and how computers are used. Therefore, contextual information necessary to understand the evidence also falls within the scope of the warrant.

VI. SEARCH METHODOLOGY TO BE EMPLOYED

21. The SUBJECT PHONE has been seized for an off-site search for evidence that is described in Attachment B of this warrant. Consistent with the information provided within this affidavit, contextual information necessary to understand the evidence, to identify the user/possessor of the child pornography, and to establish admissibility of the evidence in subsequent legal proceedings will also be sought by investigative agents.

22. Additional techniques to be employed in analyzing the SUBJECT PHONE will include (1) surveying various file directories and the individual files they contain; (2) opening files to determine their contents; (3) scanning storage areas; (4) performing key word searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are likely to appear in the evidence described in this affidavit

and its attachments; and (5) performing any other data analysis techniques that may be necessary to locate and retrieve the evidence described in this affidavit and its attachments.

23. Because it is expected that SUBJECT PHONE may constitute (1) instrumentality of the offense, (2) fruit of criminal activity, (3) contraband, or (4) evidence otherwise unlawfully possessed, it is anticipated that such evidence will not be returned to the owner and that it will be either forfeited or ultimately destroyed in accordance with the law at the conclusion of the case. However, if after careful inspection, investigators determine that the SUBJECT PHONE does not contain (1) instrumentality of the offense, (2) fruit of criminal activity, (3) contraband, (4) evidence otherwise unlawfully possessed, or (5) evidence of the person who committed the offense and under what circumstances the offense was committed, then such items seized will be returned.

VII. CONCLUSION

24. Based upon the forgoing, the undersigned respectfully submits that there is probable cause to believe that evidence, fruits and instrumentalities of violations of Title 18, United States Code Sections 2252A(a)(2)(A) and 2252A(a)(5)(B), as specifically described in Attachment B to this application, are presently located within the SUBJECT PHONE. The undersigned therefore respectfully requests that the attached warrant be issued authorizing a search for the items listed in Attachment B within the SUBJECT PHONE, which is described in Attachment A to this application.

25. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711, 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, this Court is a District Court of the United States that has jurisdiction over the offenses being investigated. 18 U.S.C. § 2711(3)(A)(i).

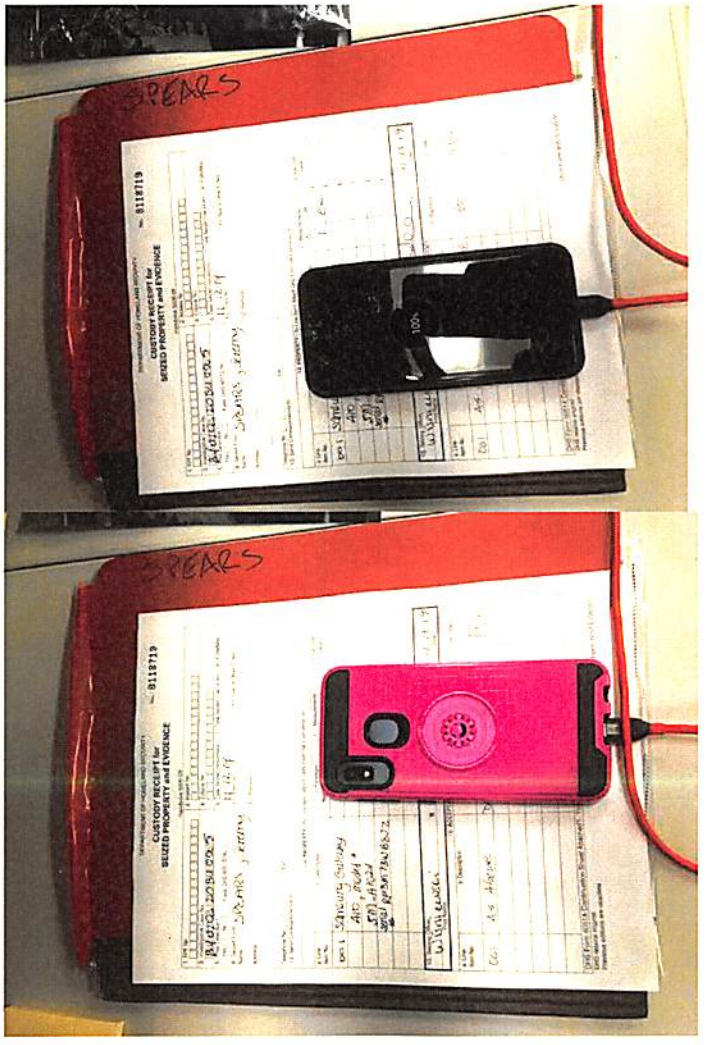
Karen L. Wisniewski, Special Agent
Homeland Security Investigations

Sworn to before me this 9th day of December, 2019

Jeremiah J. McCarthy
United States Magistrate Judge

ATTACHMENT A

a. Samsung Galaxy cellular telephone, serial number RF8M73W5EJZ, which is currently in the custody of Homeland Security Investigations' Forensic Laboratory, 250 Delaware Avenue, 8th floor, Buffalo, NY.



ATTACHMENT B

ITEMS TO BE SEARCHED FOR AND SEIZED

a. Visual depictions, including still images, videos, films or other recordings, of child pornography or minors engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256, and any mechanism used for the production, receipt, distribution, advertisement, or storage of the same;

b. Records, correspondence, evidence and data contained on SUBJECT PHONE pertaining to the production, possession, receipt or distribution of child pornography, in any form, as defined in 18 U.S.C. §2256(8), and the enticement of minors, in any form;

c. Information pertaining to or related to an interest in child pornography or the visual depiction of the sexual exploitation of a child, including any and all documents, records, images, videos, emails, email software, associated email addresses, email address book contents, internet history, browsing history, internet search history, cookies, deleted files, bookmarked and favorite web pages, user typed web addresses, desktop shortcuts, path and file names for files opened through any media and/or image viewing software, chat software, chat files, chat logs, chat names used, peer to peer software, peer to peer files, newsgroup postings by the user, IP addresses assigned, and other evidence pertaining to the possession of child pornography;

d. Documents and records contained on the SUBJECT PHONE regarding the ownership and/or possession of the searched property;

e. Records and data relating to the identification of Internet Service Provider accounts;

f. Records and data showing the identity of any user of the SUBJECT PHONE and any digital device connected to or associated with the SUBJECT PHONE; and

g. During the course of the search, photographs of the item referenced in Attachment A may also be taken to record the condition thereof and/or the location of items therein.